UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GBM Global Holding Company Limited *Plaintiff,* v. The Unidentified Individuals Listed On Schedule A, *Defendants*	Case No. 1:21-cv-06284 **DECLARATION OF WEI LI IN SUPPORT OF PETITION FOR TEMPORARY RESTRAINING ORDER IN AID OF ARBITRATION**

I, **WEI LI,** declare as follows:

1. I am a technical lead of BitMart, an exchange owned and operated by GBM Global Holding Company Limited (the "**Company**") which is the Plaintiff in the captioned matter. The Company is fully familiar with the facts asserted herein.

2. This declaration is based on my personal knowledge of the facts stated herein or on business records that were made at the time in the regular course of business. If called as a witness, I could and would testify to the statements made herein.

3. A blockchain is a type of digital database in ledger form. With blockchain technology, information is collected together in groups or blocks and linked together to create a chain of data (the "**Blockchain**").

4. In cryptocurrency trading, this "blockchain" is used to record approved transfers of digital currencies and the mining of crypto coins or tokens. Generally, a new "block" on the chain

is created by a "miner" solving complex computational math problems using a stack of computing power. Each new block must then be validated by a consensus of "nodes" or computers attached to the blockchain network that will then verify that the miner's solution to the math problem is correct. Once validated, the newly mined block will be added to the existing blockchain.

5. Transactions of a given blockchain's tokens are recorded in these blocks as they are mined at regular intervals and locked into the chain as the blocks with transaction information is validated by miners. For their mining work, the miners receive the native cryptocurrency of the given blockchain as their rewards —for example Bitcoin.

6. A malicious attack, known as a "51% attack", was carried out against the Bitcoin Satoshi Vision ("**BSV**") token network on July 9, 2021. A 51% attack occurs when one or more miners take control of more than 50% of the blockchain network's mining power or hashing power. This essentially gives them control of the network because these miners with majority control can now form the majority "consensus" of nodes and dictate what cryptocurrency transactions are recorded on the next block on the blockchain. With such control, these malicious miners can carry out a malicious "block reorganization."

7. A block reorganization occurs when the miners with control of the network remove ***previously validated*** blocks from the blockchain. Theoretically, a group of miners with 51% of the mining power should have a higher probability of mining and adding new blocks to the blockchain faster than other miners. These miners can then reorganize the chain by setting up a new, private, chain in parallel to the existing one, and start mining on it.

8. Because the blockchain protocol is designed such that newly mined blocks are added to the longest validated chain when separate versions exist simultaneously, a "fork" in the blockchain can become— for as long as the malicious hackers have control, a dominant version of

the blockchain recording different transactions from the legitimate one. The miners with majority control of the network can then double spend by transacting on the newly dominant "fork," erasing the transaction from the record, and making the same transactions a second time.

9. The BSV token blockchain appears to be more susceptible to such 51% attacks because statistics show that a mining pool (a syndicate or cartel of miners) called Taal currently commands well over 51% of the network's mining power. Without going into details, such concentration makes the BSV network highly susceptible to 51% attacks.

10. This vulnerability is exacerbated by the fact that the BSV network only has a total of about 190 active nodes, whereas other cryptocurrencies have much more. Bitcoin, for example, currently has over 83,000 active nodes. This means that less mining power is needed to temporarily gain majority control of the BSV network as compared to Bitcoin network.

11. In this instance, malicious actors successfully carried out a 51% attack on the BSV blockchain on July 9, 2021 and briefly took over the network. During this time, they manipulated and "mined" "fake" BSV tokens on a forked, private, chain and deposited them into 92 accounts they opened with BitMart. The hackers recorded these transactions on the private chain created and successfully deposited these "fake" BSV tokens to BitMart to trade for other legitimate cryptocurrencies that held value, thus "cashing out".

12. BitMart confirmed the "fake" BSV token deposits at the time because these tokens came from the private chain that was the longest, briefly dominant chain at the time, which is generally a marker that the blockchain can be trusted.

13. The BitMart exchange only confirms each deposit after 2 blocks are validated by the blockchain network. This typically takes around 10 minutes. In that 10-minute window, so long as the private chain remains longer than the main chain, the exchange will recognize the

longer chain as the correct blockchain and the deposited cryptocurrency which is recorded in the then-longer private chain is then confirmed by the exchange.

14. Eventually, as the hackers stop mining on the private chain and abandon it, the main chain will grow longer than the private chain again, and the BSV network will recover from the attack by switching back to the main chain. At that juncture, the legitimate BSV network will then roll back the previous transactions that were recorded on the private chain, thus ceasing to recognize the "fake" BSV tokens that were mined on that private chain.

15. The moment BitMart found out about the attack, it undertook efforts to trace the stolen assets and unravel the hack. BitMart has contacted a security company, named SlowMist, who is attempting to track down as many of the stolen cryptocurrencies as possible. BitMart has also contacted XRPEXPLORER, the official xrp blockchain explorer, to help us to trace these cryptocurrencies.

I declare under penalty of perjury that the foregoing is true and accurate to the best of my knowledge, information, and belief.

Signed July 23, 2021.

/s/ *Wei Li*

_____

Wei Li
Hangzhou, China